ISSN: 2349-0845

IJRST

International Journal of Research in Science & Technology (IJRST)
Volume 1, Issue 2 : March 2014
www.ijrst.weebly.com

Using Advanced Encryption Standard (AES) Algorithm Upgrade the Security Level of ATM Banking Systems

Mrs. Sonali S. Ingle, Mrs. Pratima M. Bhalekar, Mrs. Ketaki S. Pathak

Asst. Professor, Computer Science Department at Ashoka Center for Business and Computer Studies, Nashik, Maharashtra, India.

Asst. Professor, Computer Science Department at Ashoka Center for Business and Computer Studies, Nashik, Maharashtra, India.

Asst. Professor, Computer Science Department, RNC Arts, JDC Commerce, NSC Science College, Nashik, Maharashtra, India

Abstract

Biometric ATM are used for wide range of applications like for Banking, Coupons & Self service ATM. Biometrics ATM offer ATM type interface along with at-least one Biometrics capture device like Fingerprint Scanner, Iris camera, Palm/Finger Vein scanner , Face recognition camera. They are often called Multi-Biometrics ATM, Wall mount Biometrics ATM, Biometrics Devices / Machine.Most of the ATM in the past has been using ID cards to identify users but with the wide acceptance of Biometrics, a new generation of Biometrics ATM is being deployed for wide range of applications worldwide.

We are introducing you an embedded Crypto-Biometric authentication scheme for ATM banking systems. In this scheme, cryptography and biometric techniques are fused together for person authentication to ameliorate the security level. The fingerprint template including singular points, frequency of ridges and minutiae are stored at the central banking server when enrollment. At the time of transaction fingerprint image is acquired at the ATM terminal using high resolution fingerprint scanner. The fingerprint image is enhanced and then encrypted using 128 bit private key algorithm. The encrypted image is transmitted to the central server via secured channel. At the banking terminal the image is decrypted using the same key. Based on the decrypted image, minutiae extraction and matching are performed to verify the presented fingerprint image belongs to the claimed user. The authentication is signed if the minutiae matching are successful. The proposed scheme is fast and more secure. Computer simulations and statistical analysis are presented.

Keywords: Biometrics, Fingerprint, Verification, Cryptography, Encryption, Decryption and Symmetric key algorithms.

I. INTRODUCTION

Biometrics technology measures an individual's unique physical or behavioral characteristics, such as fingerprints, facial characteristics, voice pattern, and gait, to recognize and confirm identity". This makes the data more secure and biometrics options are becoming more efficient than personal PINs. Biometric technology is often combined innovations such as smart cards.

Biometric authentication mechanisms are receiving a lot of public attention. A biometric device is perhaps the ultimate attempt in trying to prove who you are. Biometrics based authentication is a potential candidate to replace password-based authentication. Among all the biometrics, fingerprint based identification is one of the most mature and proven technique. Cryptography provides the necessary tools for accomplishing secure and authenticated transactions. It not only protects the data from theft or alteration, but also can be used for user authentication. In a conventional cryptographic system, the user authentication is possession based. The weakness of such authentication systems is that it cannot assure the identity of the maker of a transaction; it can only identify the maker's belongings (cards) or what he remembers (passwords, PINs etc.) Automatic biometric authentication is an emerging field to address this problem. Fingerprint authentication is the most popular method among biometric authentication. However, it is infeasible to encrypt such a large volume of image using conventional cryptography for the purpose of centralized fingerprint matching. A strong interest in biometric authentication is to integrate encryption key with biometrics.

The project aims at developing a novel crypto-biometric authentication scheme in ATM banking systems. It mainly reduces the accessing time, when compared with manual based banking system. ATMs are now a normal part of daily life, it explores the accessibility barriers that ATMs present to people with a variety of disabilities, particularly examining the access barriers experienced by the people who are blind, vision impaired or who have reading, learning or intellectual disabilities.

Together with the development of biometric authentication, integrated biometrics and cryptosystems has also been addressed. Biometric authentication in our paper is image based. For remote biometric authentication, the images need to be encrypted before transmitted. The permutation of pixels, the substitution of gray level values, and the diffusion of the discredited map can encrypt an image effectively.

In this paper, an embedded crypto-biometric authentication protocol is proposed. The fingerprint image acquired from the user is encrypted in the ATM terminal for authentication. The encrypted image is then transmitted over the secured channel to the central banking terminal. In the banking terminal fingerprint image is decrypted. The decrypted image is compared with the fingerprint templates. The authentication is valid if the minutiae matching are successful.

The organization of the paper is given as follows: Section 2 deals with description of the new embedded crypto-biometric authentication protocol. Section 3 provides the concepts of Encryption and Decryption algorithms. Generation of encryption key is studied in Section 4. Simulation and evaluation of the encryption scheme is conducted in Section5. Conclusions are presented in Section 6.

2. EMBEDDED CRYPTO-BIOMETRIC AUTHENTICATION PROTOCOL

Generally, there are two basic fingerprint authentication schemes, namely the local and the centralized matching. In the central matching scheme, fingerprint image captured at the terminal is sent to the central server via the network and then it is matched against the minutiae template stored in the central server.

There are three stages in the protocol namely registration, login and authentication. In the registration phase, the fingerprints of ATM users are enrolled and the derived fingerprint templates are stored in the central server. The login phase is performed at an ATM terminal equipped with a fingerprint sensor. The proposed block schematic of embedded crypto biometric authentication system is shown in Fig (1).

In the authentication phase, the fingerprint image is then encrypted and transmitted to central server via secured channel. At the banking terminal the image is decrypted using 128 bit private key algorithm. The encrypted image is transmitted to the central server via secured channel. At the banking terminal the image is decrypted using the same key. Based on the decrypted image, minutiae extraction and matching are conducted to verify the presented fingerprint image belongs to the claimed user. The authentication is signed if the minutiae matching are successful.

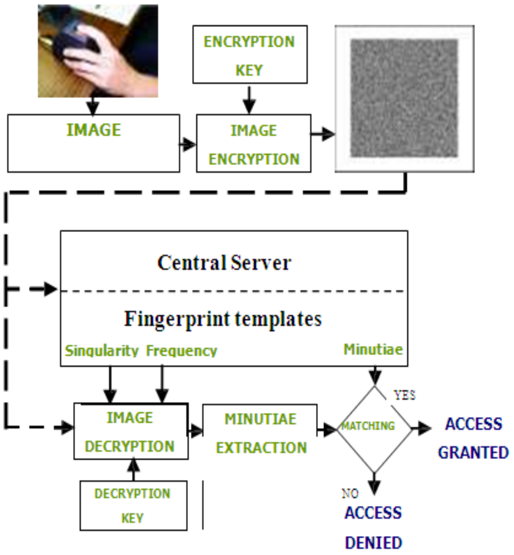
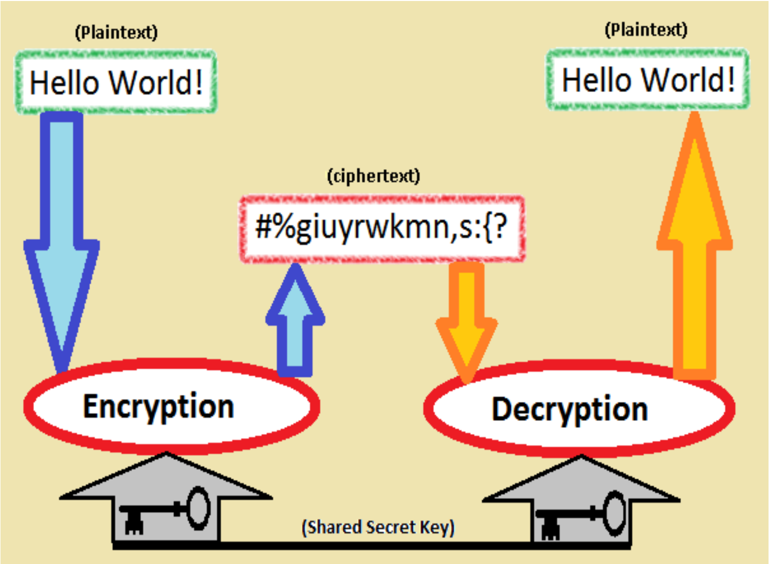


Fig. 1 Schematic of embedded crypto biometric authentication system.

3. ENCRYPTION AND DECRYPTION ALGORITHMS



Encryption is the process of converting plain image into cipher image. Plain image in our paper is the unsecured form of fingerprint image. By using the appropriate keys, plain image is encrypted into cipher image before transmitting through the secured channel.

Decryption is the reverse process of encryption. Fingerprint image is recovered (plain image) by using the same key. DES, Triple DES and AES algorithms are the commonly used symmetric key algorithms. Shared key, less time consumption, easy operation and secret key are the merits of symmetric key algorithms.

3.1 Advanced Encryption Standard (AES) Algorithm

The advanced encryption standard (AES) is a replacement to DES as the federal standard. AES has already received widespread use because of its standard definition, high security and freedom patent entanglements. In cryptography, the Advanced Encryption Standard (AES) is also known as Rijndael algorithm.

Unlike its predecessor DES, Rijndael is an iterated block cipher which supports variable block length and key length. Both lengths can be independently specified as 128, 192 or 256 bits. It has a variable number of iterations: 10, 12 and 14 for key lengths of 128, 192 or 256 bits respectively. In this paper, a 128 bit block [14] and key length are assumed, although the design could be adopted without difficulty to other block and key lengths. AES is fast in both software and hardware, relatively easy to implement, and requires little memory. As a new encryption standard, it is currently being deployed on a large scale.

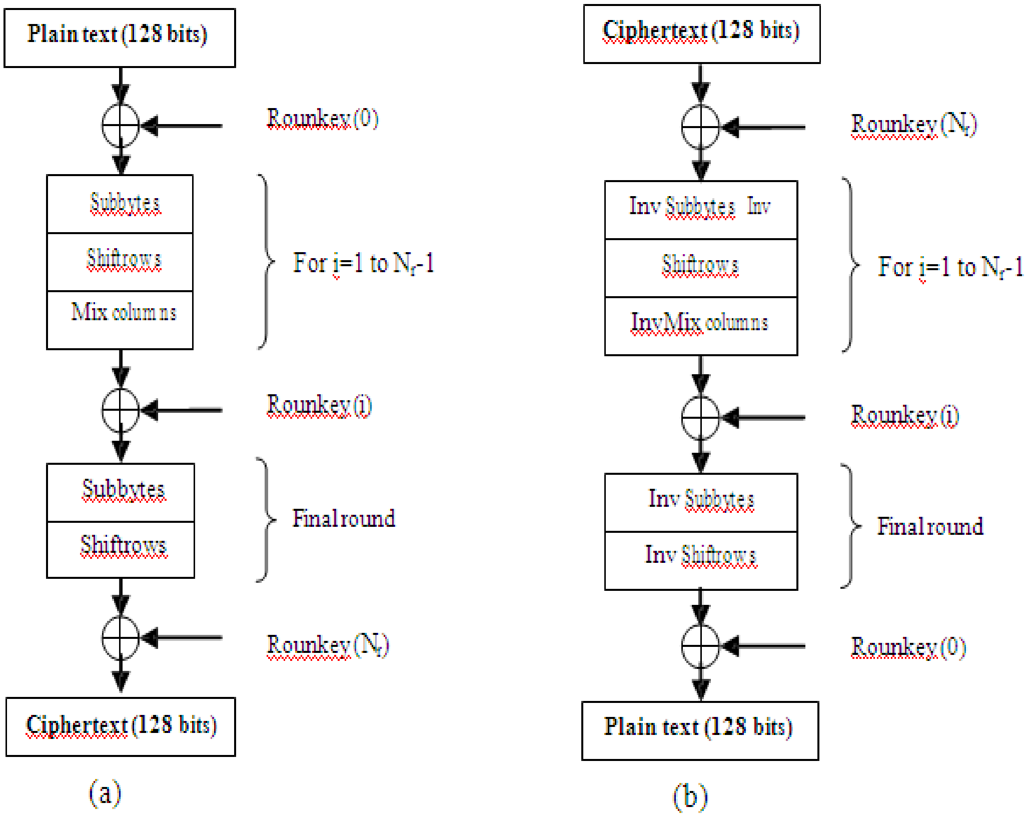


Fig. 2 AES algorithm (a) Encryption Structure (b) Decryption Structure

AES [14] consists of following steps

- Key Generation
- Initial Round
- Rounds

(i) Sub Bytes — a non-linear substitution step where each byte is replaced with another according to a lookup table.

(ii) Shift Rows — a transposition step where each row of the state is shifted cyclically a certain number of steps.

(iii) Mix Columns — a mixing operation which operates on the columns of the state, combining the four bytes in each column.

(iv) AddRoundKey — each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

- Final Round (no Mix Columns)

4. SIMULATION, STATISTICAL AND STRENGTH ANALYSIS

We have proposed in this section encryption scheme is tested. Simulation results and its evaluation are presented.

4.1 Simulations

The gray level fingerprint image is shown Fig.3(a). The first 3D permutation is performed with the key {32, 21, 0, 18, 35, 5, 15, 14, 9, 16, 12, 4, 18, 21, 6, 30}. After first round of 3D permutation, the encrypted fingerprint image is shown in Fig.3(b). The second round permutation is performed with the key {7, 16, 20, 12, 4, 8, 13, 8, 9, 39, 28, 27, 1, 16, 50, 42}. After that, the image is shown in Fig.3(c). The third round permutation is finished with a key {1, 23, 8, 19, 32, 3, 25, 12, 75, 31, 4, 10, 14, 5, 25, 13}. After this, the image is shown in Fig.3(d), which is random looking.

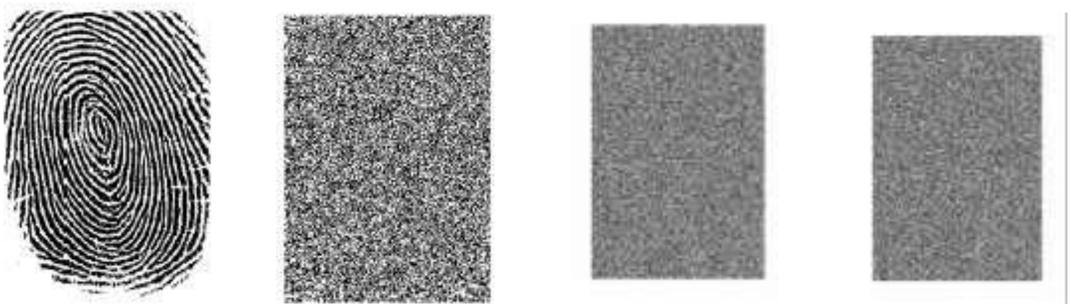


Fig. 3 Fingerprint and the encrypted image. (a) Original image; (b) One round of iteration; (c) Two rounds of iterations; (d) Three rounds of iterations.

4.2 Statistical and Cryptographic Strength Analysis

- Statistical analysis.

The histogram of original fingerprint image is shown in Fig.4 (a). After 2D chaotic mapping, the pixels in fingerprint image can be permuted, but as the encrypted fingerprint image has the same gray level distribution and same histogram as in Fig.4 (a). As introduced in Section 4, 3D chaotic map can change the gray level of the image greatly. After one round and three rounds of 3D substitution, the histograms are shown in Fig.4(b) and (c) respectively, which is uniform, and has much better statistic character, so the fingerprint image can be well hidden.

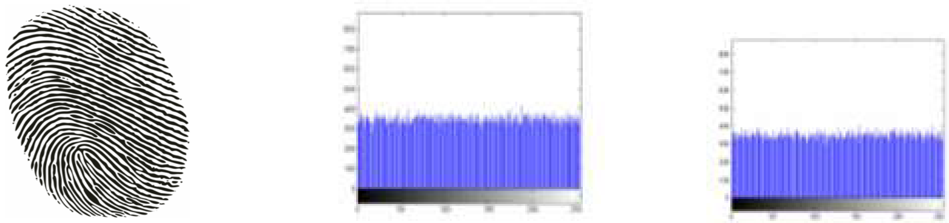


Fig. 4 Histograms of fingerprint image and the encrypted image. (a) Original fingerprint image; (b) One round of 3D iteration; (c) Three rounds of 3D iterations.

• Strength analysis.
The cipher technique is secure with respect to a known plaintext type of attack. With the diffusion methodology, the encryption technique is safe to cipher text type of attack. As the scheme proposed in this paper use different keys in different rounds of iterations, and the length is not constrained, it can be chosen according to the developer's need.

5. CONCLUSION

An embedded Crypto-Biometric authentication scheme for ATM banking systems has been proposed. The claimed user's fingerprint is required during a transaction. The fingerprint image is encrypted via 3D chaotic map as soon as it is captured, and then transmitted to the central server using symmetric key algorithm. The encryption keys are extracted from the random pixel distribution in a raw image of fingerprint, some stable global features of fingerprint and/or from pseudo random number generator. Different rounds of iterations use different keys.

At the banking terminal the image is decrypted using the same key. Based on the decrypted image, minutiae extraction and matching are performed to verify the presented fingerprint image belongs to the claimed user. Future work will focus on the study of stable features (as part of encryption key) of fingerprint image, which may help to set up a fingerprint matching dictionary so that to narrow down the workload of fingerprint matching in a large database.

REFERENCES

[1] Jain, A.K., Prabhakar, S., Hong, L., Pankanti, S.:Filterbank-based fingerprint matching, *IEEE Trans. on Image Processing*, 9 (2000) 846-859

[2] Chen, G., Mao, Y., Chui, C.: A symmetric encryption scheme based on 3D chaotic cat map, *Chaos, Solitons & Fractals*, 21 (2004) 749-761

[3] J. Daemen, V. Rijmen, ``the Block Cipher Rijndael," Smart Card Research and Applications, LNCS 1820, J.- J. Quisquater and B. Schneier, Eds., Springer-Verlag, 2000, pp. 277-284.

[4] Ratha, N.K, Karu, K. Chen, S., Jain, A.K.: A real-time matching system for large fingerprint databases, IEEE Trans. on Pattern Anal. Machine Intell., 18 (1996) 799- 813

[5] Fridrich, J.: Symmetric Ciphers Based on two dimensional chaotic maps, *Int. J. Bifurcation and Chaos*, 8 (1998) 1259-1284.

[6] J. Daemen and V. Rijmen, ``Rijndael, the advanced encryption standard," Dr. Dobb's Journal, Vol.~26, No.~3, March 2001, pp.~137--139.

[7] F.Han, J.Hu, X.Yu, Feng, Zhou: A novel hybrid cryptobiometric authentication scheme for ATM based banking applications, Springer-Verlag Berlin Heidelberg, (2005) 675-681.

[8] Cryptography and network Security-Atul Kahate.